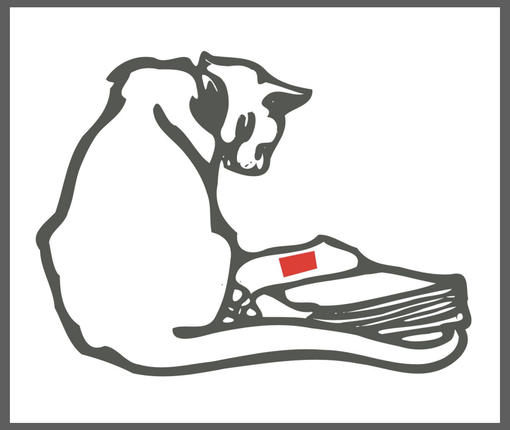


CyCAT

An Open and Public Cybersecurity Resource Catalogue

Official Launch. Alexandre Dulaunoy, Saâd Kadhi and the CyCAT team

EU ATT&CK Community - 1st June
TLP:WHITE

CyCAT?

What, Who, Why

Welcome to the jungle

- Cyberattacks are continuously increasing, in number, complexity and variety
- To defend their constituencies, defenders have launched several initiatives
- Numerous tools, products, frameworks and methodologies to prevent, detect and respond to these threats
- Not always properly tested, not always easy to locate, produced in a highly decentralised fashion
- And the rhythm is accelerating
- With little consideration to prior art (mainly due to lack of knowledge?)

Where should I start?

- I need to defend my constituency
- What tools, rules, playbooks, controls,… exist out there?
- Which ones are the most relevant for my context & for my current maturity?
- Which ones work best for my needs?
- Which ones have been sufficiently tested?
- Which ones supersede, augment or conflict with existing ones?
- Which ‘resource producers’ tend to make quality products for my needs?

Enters CyCAT

- CyCAT = **CY**bersecurity Resource **CAT**alogue
- Non-profit and public initiative trying to solve a (cyber)age-old problem
- Map + document, in a single formalism, and catalogue all the available…
- Cybersecurity tools, rules, playbooks, controls…
- Contextualised to facilitate searching and selection
- Resource interlinking to support the creation of coherent ‘packages’
- ‘Packages’ = plug-and-play solutions for less-mature entities

The CyCAT System

High-level concepts

Mantra of the CyCAT System

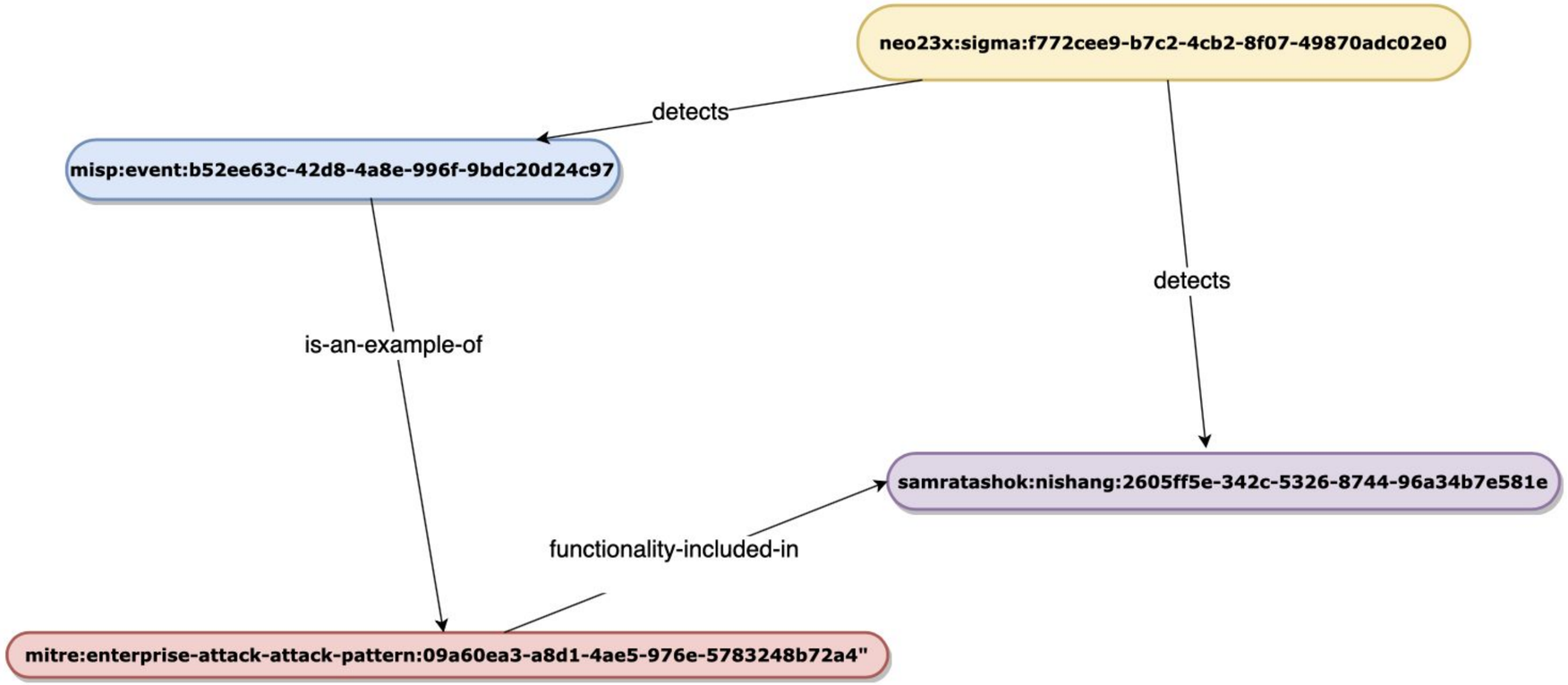
- A simple data model
- Be open on the crawling
- **Public and Open API** (everybody hates private/restricted API)
- **Fast lookup**
- Everyone can rebuild the CyCAT directory for local or custom lookup (everything at CyCAT is **open source**)
- Ensure **freedom of each publisher**

CyCAT API and back-end

- API (https://api.cycat.org/) where you can freely lookup by **UUID, namespace/id**, **relationships** and **keywords**
- Building on the success of initiatives such as CVE and elegant solutions such as MISP's UUID or MITRE ATT&CK® ID
- CyCAT is **crawling known repositories**
- For more information: https://github.com/CyCat-project/cycat-service and API documentation
- Don't forget to join us Today at 17:30 CEST for a quick API demo

URL example

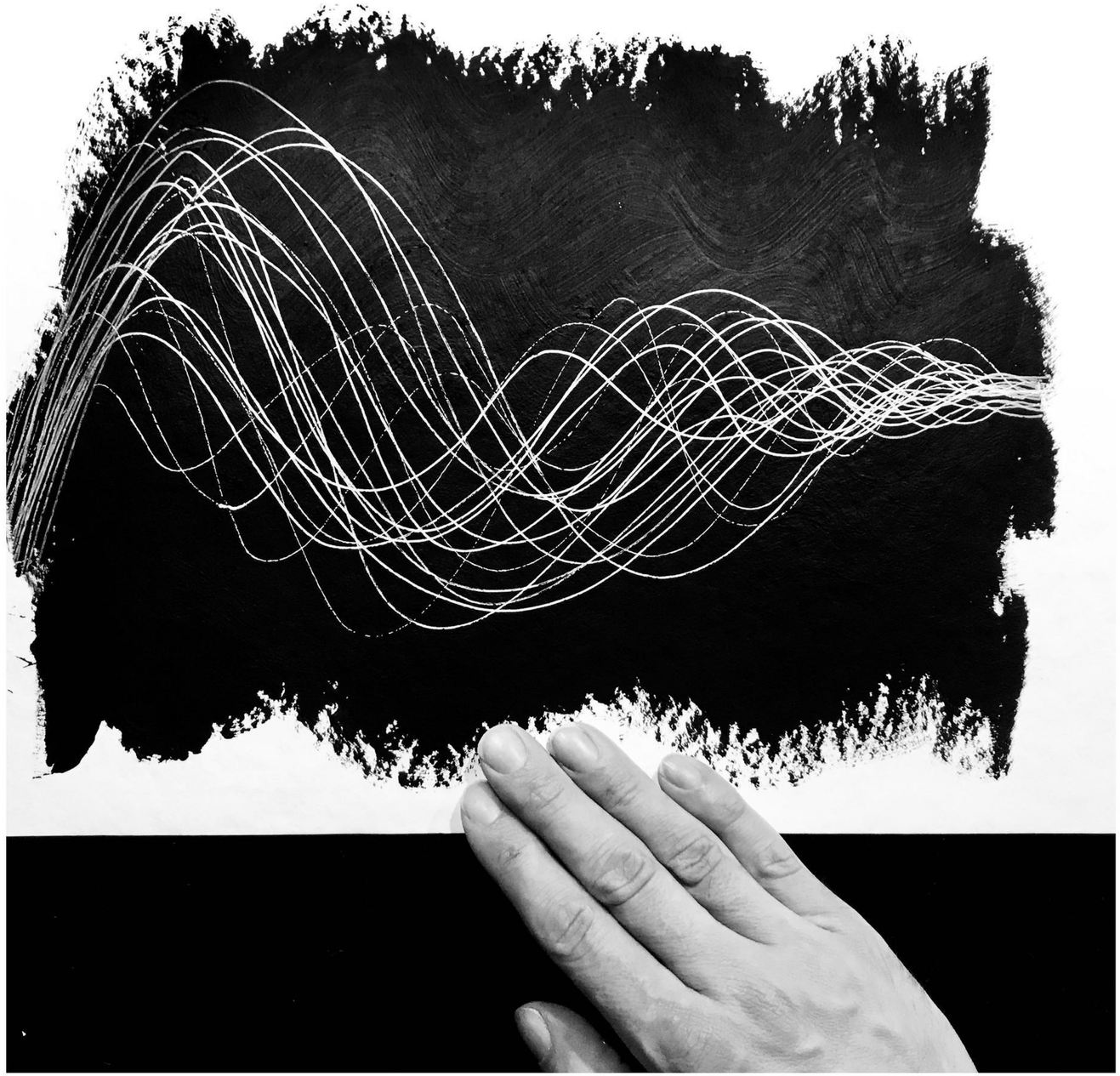
An CyCAT example with nishang, an offensive powershell




```
% uuidgen --sha1 -n "690b3b43-d689-481c-aa61-5351963a36f2" -N "samratashok:nishang:"
2605ff5e-342c-5326-8744-96a34b7e581e
```

The Initiative

And why we need your help



Current status and next steps

- CyCAT was launched on 1st February 2021
- By Freddy Dezeure, Alexandre Dulaunoy, Andras Iklody and Saâd Kadhi
- We received excellent suggestions and questions from key community contributors: Patrick Bareiss, John Lambert, Thomas Patzke, John Wunder, Daniil Yugoslavskiy…
- Today, we released a first version 0.9 of the public API (https://api.cycat.org/) with 9700+ items including relationships, producer name spaces and links from ATT&CK, MISP public feeds, MISP galaxy clusters, SigmaHQ rules.

CyCAT needs you

- This is an ambitious project
- .. without your help and the help of the community they love and care for
- There are still many questions we need to address and some difficult problems we need to solve
- Publisher, defender, both? Read the White Paper, look at the taxonomy, go through the FAQ and contribute
- Got questions or suggestions? ➡️ info@cycat.org
- The easy way if you want to contribute “**add unique identifiers such as UUIDs in your projects and publish it in machine parseable format (JSON, YAML)**”